Universität Tübingen, WS 13/14

Bernd Borchert

Übungen Kryptologie

Blatt 4.

Aufgabe 1. Führen Sie die AES Bijektion B, also nacheindander die Bijektionen SubBytes, ShiftRows, MixColumns, auf folgender Eingabe aus:

00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f

Verwenden Sie die in den Folien angegebenen Tabellen.

Aufgabe 2. Die Elemente von GF(2^8) können als Polynome der Form

$a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$

angesehen werden, wobei alle a_1 entweder 0 oder 1 sind, und die Addition + das EXOR ist, d. h. $x^i + x^i = 0$.

Multiplizieren Sie die Polynome $x^7 + x^3 + x^2 + 1$ und $x^5 + x + 1$, und teilen Sie dann das Ergebnis durch das den Körper GF(2^8) definierende irreduzible Polynom $x^8 + x^4 + x^3 + x + 1$.

Das Polynom $a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ kann auch als Binärzahl $a_7\,a_6\,a_5\,a_4\,a_3\,a_2\,a_1\,a_0$ angesehen werden. Was ist also$141 \cdot 35$ im Körper GF(2^8)?

Aufgabe 3. Ein rechteckiger Teil des Bildschirmsignals ist verschlüsselt und wird durch ein Entschlüsselungsgerät dekodiert, das zwischen Bildschirmausgang und Bildschirm geschaltet wird. Die AES256 Entschlüsselung der zeilenweise eingehenden Pixel-Farbwerte findet nicht durch einen Prozessor statt, sondern durch eine Hardwareschaltung, die unter anderem 15 Teil-Schaltungen hat, die jeweils eine Runde von den 15 Runden des AES256 implementieren.

(a) Machen Sie durch eine kurze Skizze klar, dass man AES “pipelinen” kann, d.h., man kann schon mit der Entschlüsselung des 2. Farbwert-Substrings beginnen, wenn die erste Runde der Entschlüsselung des 1. Farbwert-Substrings fertig ist, uns so weiter. (Für die Abwicklung von 50 bis 100 Bildschirmsignalen in der Sekunde ist dieses pipelining sogar wesentlich.)

(b) Skizzieren Sie kurz, dass gerade bei Bildern das bekannte Problem besteht, bei AES ohne feedback (also im EBC-Modus) zu arbeiten.

(c) Weil das Rechteck eventuell nur klein ist, kann in der ersten Zeile, die für die Verwaltung vorgesehen ist, nur ein kurzer seed von nicht mehr als 10 Byte stehen. Es reicht also gerade für ein feedback für die erste AES-Berechnung – wo bekommen die weiteren (gepipelineten) AES-Berechnung 2 bis 15 ihren feedback her? (die 16. könnte den der 1. nehmen) Welchen feedback Modus schlagen Sie vor? Was sollten Sie aus Sicherheitsgründen nicht tun?